What is claimed is:

1. A method comprising:

determining at a first location if a classification parameter is available for Internet Protocol security (IPsec) traffic that indicates a route for the IPsec traffic;

if a classification parameter is not available, decrypting the IPsec traffic at a second location if the IPsec traffic is encrypted and determining the classification parameter for the IPsec traffic at the second location; and

forwarding the IPsec traffic based on the classification parameter.

2. The method of claim 1 further comprising receiving the IPsec traffic at the first location.

3. The method of claim 1 in which the classification parameter includes a security parameter index (SPI) associated with the IPsec traffic.

4. The method of claim 1 in which the IPsec traffic includes a data packet.

5. The method of claim 1 further comprising forwarding other IPsec traffic included in a traffic stream with the IPsec traffic based on the classification parameter.

6. An article comprising:

a machine-readable medium which stores machine-executable instructions, the instructions causing a machine to:

determine at a first mechanism if a classification parameter is available for Internet Protocol security (IPsec) traffic that indicates a route for the IPsec traffic;

if a classification parameter is not available, decrypt the IPsec traffic at a second mechanism if the IPsec traffic is encrypted and determine the classification parameter for the IPsec traffic at the second mechanism; and

forward the IPsec traffic based on the classification parameter.

7. The article of claim 6 further causing a machine to receive the IPsec traffic at the first mechanism.

8. The article of claim 6 in which the classification parameter includes a security parameter index (SPI) associated with the IPsec traffic.

9. The article of claim 6 in which the IPsec traffic includes a data packet.

10. The article of claim 6 further causing a machine to forward other IPsec traffic included in a traffic stream with the IPsec traffic based on the classification parameter.

11. A system comprising:

a first mechanism configured to communicate with a network, to determine if a classification parameter that indicates a route for a traffic stream is available for a packet included in the traffic stream; and

a second mechanism configured to receive the packet from the first mechanism, to perform an encryption procedure on the packet if the packet is encrypted and associated with a known encryption-related key, and, if the classification parameter is available, to forward the packet based on the route for the traffic stream.

12. The system of claim 11 further comprising a third mechanism configured to communicate with the first mechanism and with the second mechanism and to determine a classification parameter for the packet if a classification parameter is not available.

13. The system of claim 12 in which the second mechanism is also configured to forward the packet to the third mechanism if the packet is not associated with a known encryption-related key.

14. The system of claim 12 in which the third mechanism is also configured to, after determining the classification

parameter for the packet, forward the classification parameter to the first mechanism.

15. The system of claim 12 in which the third mechanism is also configured to, after determining the encryption-related key for the packet, forward the encryption-related key to the second mechanism so that the second mechanism can perform the encryption-related procedure.

16. The system of claim 12 in which the second mechanism and the third mechanism are both included as part of a fourth mechanism.

17. The system of claim 11 further comprising a plurality of additional mechanisms, each additional mechanism configured to communicate with the first mechanism, to perform an encryption procedure on the packet if the packet is encrypted and associated with a known encryption-related key, and, if the classification parameter is available, to forward the packet based on the route for the traffic stream.

18. The system of claim 11 in which the packet includes an Internet Protocol security data packet.

19. The system of claim 11 in which the traffic stream includes a plurality of Internet Protocol security data packets.

20. The system of claim 11 in which the first mechanism is also configured to forward the packet to the second mechanism if the packet is encrypted.

21. The system of claim 11 in which the route for the traffic stream includes a route through a network.

22. The system of claim 21 in which the network includes an Internet.

23. The system of claim 11 in which the encryption procedure includes encrypting the packet.

24. The system of claim 11 in which the encryption procedure includes decrypting the packet.

25. The system of claim 11 further comprising another mechanism configured to receive the packet from the second mechanism and to forward the packet based on the route to an ultimate destination of the packet.

26. The system of claim 11 in which the first mechanism is also configured to route packets included in the traffic stream based on a load balancing scheme.